Jennifer Lynch (SBN 240701)
jlynch@eff.org
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Telephone: (415) 436-9333
Facsimile: (415) 436-9993

David L. Sobel *(pro hac vice pending)*
sobel@eff.org
ELECTRONIC FRONTIER FOUNDATION
1818 N Street, N.W.
Suite 410
Washington, DC 20036
Telephone: (202) 797-9009 x104
Facsimile: (202) 707-9066

Attorneys for Plaintiff
ELECTRONIC FRONTIER FOUNDATION

UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

LB

CV 13 2946

ELECTRONIC FRONTIER FOUNDATION,

Plaintiff,

v.

DEPARTMENT OF JUSTICE,

Defendant.

COMPLAINT FOR INJUNCTIVE RELIEF FOR VIOLATION OF THE FREEDOM OF INFORMATION ACT, 5 U.S.C. § 552

1. This is an action under the Freedom of Information Act (FOIA), 5 U.S.C. § 552, for injunctive and other appropriate relief. Plaintiff seeks the release of records that Plaintiff requested from Defendant Department of Justice and its component, Federal Bureau of Investigation, concerning the agency's efforts to build out its biometrics systems and specifically its face recognition capabilities.

PARTIES

2. Plaintiff Electronic Frontier Foundation (EFF) is a not-for-profit corporation established under the laws of the Commonwealth of Massachusetts, with offices in San Francisco, California and Washington, DC. EFF is a donor-supported membership organization that works to inform policymakers and the general public about civil liberties issues related to technology and to act as a defender of those liberties. In support of its mission, EFF uses the FOIA to obtain and disseminate information concerning the activities of federal agencies.

3. Defendant Department of Justice (DOJ) is a Department of the Executive Branch of the United States Government. DOJ is an "agency" within the meaning of 5 U.S.C. § 552(f). The Federal Bureau of Investigation (FBI) is a component of Defendant DOJ.

JURISDICTION

4. This Court has both subject matter jurisdiction over this action and personal jurisdiction over the parties pursuant to 5 U.S.C. §§ 552(a)(4)(B) and 552(a)(6)(C)(i). This Court also has jurisdiction over this action pursuant to 28 U.S.C. § 1331.

VENUE AND INTRADISTRICT ASSIGNMENT

5. Venue is proper in this district under 5 U.S.C. § 552(a)(4)(B) and 28 U.S.C. § 1391(e).

6. Assignment to the San Francisco division is proper pursuant to Local Rule 3-2(c) and (d) because a substantial portion of the events giving rise to this action occurred in this district and division, where Plaintiff is headquartered.

FACTUAL ALLEGATIONS

The FBI is Building "Bigger, Faster and Better" Biometrics Systems

7. The FBI has maintained a national criminal biometrics repository since 1924 and now controls one of the largest biometrics databases in the world.[1] This database, called the Integrated Automated Fingerprint Identification System (IAFIS), contains more than 100 million

[1] FBI, *Integrated Automated Fingerprint Identification System*, https://www.fbi.gov/about-us/cjis/fingerprints_biometrics/iafis/iafis (last visited June 24, 2013) (hereinafter "FBI, *Integrated Automated Fingerprint Identification System*").

fingerprints. 34 million of those are civil prints, which are collected as part of background checks for sensitive positions and from US service members, applicants for federal jobs, and others. More than 70 million of the prints in IAFIS are criminal and collected as a result of arrest, incarceration, or another criminal justice purpose.[2] The database also contains biographic data such as name, identification number and address; "criminal histories; mug shots; scars and tattoo photos; physical characteristics like height, weight, and hair and eye color; and aliases."[3]

8. For the last several years, the FBI has been working with private, federal, state and local partners to build a "bigger, faster and better"[4] biometrics system to replace IAFIS.[5] In 2008, the FBI awarded a contract estimated at 1 billion dollars to Lockheed Martin, the contractor that developed the original IAFIS, to build the new system.[6] This system, called Next Generation Identification or NGI, is designed to be "multimodal" and will eventually include many "forms of biometric identification like palm prints, iris scans, facial imaging, scars, marks, and tattoos—in one searchable system."[7] NGI is also designed to be scalable to allow it to accommodate advanced forms of biometrics like voice and gait as they become available in the future.[8]

NGI's Facial Recognition Component

9. Although IAFIS has allowed the submission of some photographs since its inception in 1999, this capability has been limited.[9] Agencies are only able to submit a limited number of criminal, "mug shot"-style photographs. These photographs are linked to the fingerprints and

---

[2] FBI, *Privacy Impact Assessment (PIA) for the Next Generation Identification (NGI) Interstate Photo System (IPS)*, (June 9, 2008) http://www.fbi.gov/foia/privacy-impact-assessments/interstate-photo-system (hereinafter "FBI, *PIA for the NGI IPS"*); FBI, *Integrated Automated Fingerprint Identification System*.

[3] FBI, *Integrated Automated Fingerprint Identification System*.

[4] FBI, *Beyond Fingerprints: Our New Identification System*, https://www.fbi.gov/news/stories/2009/january/ngi_012609 (last visited June 24, 2013) (hereinafter "FBI, *Beyond Fingerprints: Our New Identification System*").

[5] FBI, *Next Generation Identification*, https://www.fbi.gov/about-us/cjis/fingerprints_biometrics/ngi (last visited June 24, 2013).

[6] Alice Lipowicz & Ben Bain, *FBI Awards NGI Contract to Lockheed Martin*, Federal Computer Week (Feb. 12, 2008) http://fcw.com/articles/2008/02/12/fbi-awards-ngi-contract-to-lockheed-martin.aspx.

[7] FBI, *Beyond Fingerprints: Our New Identification System*.

[8] *Id.*

[9] FBI, *Integrated Automated Fingerprint Identification System*.

biographic data with which they are submitted, and, as IAFIS currently has no face recognition capabilities, the system is not able to search through the photographs independently from the prints or data. Further, FBI does not accept photographs with civil fingerprint submissions.

10. NGI will change almost everything about how the FBI treats photograph submissions. For example, NGI will allow "the increased capacity to retain photographic images, additional opportunities for agencies to submit photographic images, and additional search capabilities, including automated searches via the NCIC."[10] The proposed new system would also allow law enforcement "to collect and retain other images (such as those obtained from crime scene security cameras" and from friends and family)[11] and would allow submission of "civil photographs along with civil fingerprint submissions that were collected for noncriminal purposes."[12]

11. NGI will also apply face recognition algorithms[13] to the photographs, creating a unique "face print" for each person. This will allow users to upload a photo of an unknown person to the system, and the system will search through the database of face prints to find possible matches.

12. Since late 2011, the FBI has been working with several states as part of a pilot program to develop the face recognition capabilities of NGI.[14] The pilot program will allow participants that already have facial recognition capabilities within their own state criminal database systems to upload face recognition-ready photographs to NGI and to search through a database of mug shot photos.[15] The goals of the pilot program are to "test the facial recognition

---

[10] FBI, *PIA for the NGI IPS*.
[11] *Id.*
[12] *Id.*
[13] *See, e.g.*, FBI Biometric Center of Excellence, *Face Recognition*, http://www.biometrics.gov/Documents/FaceRec.pdf#page=2 (last visited June 24, 2013) (discussing various face recognition algorithms).
[14] *Staff Paper: Next Generation Identification (NGI) Program Implementation and Transition Update*, 6, CJIS Advisory Policy Board (APB) Spring 2012 Advisory Process Meetings https://www.eff.org/file/35292#page/6/mode/1up (last visited June 20, 2013)(hereinafter "*Staff Paper: NGI Program Implementation and Transition Update*").
[15] *Id.*

processes, resolve policy and processing issues, solidify privacy protection procedures, and address user concerns."[16]

13. As part of the pilot program, the FBI has executed Memoranda of Understanding (MOUs) with several states that already have existing "Face/Photo search capability." As of Spring 2012, these states included Maryland, Hawaii, and Michigan.[17] As of Summer 2012, other states, including South Carolina, Ohio, and New Mexico were "engaged in the MOU review process" to participate in the pilot program, while Kansas, Arizona, Tennessee, Nebraska, and Missouri had expressed interest in the program.[18]

14. Once the pilot program concludes, the FBI will roll out NGI access to states that do not already have their own face recognition capabilities.[19] The FBI appears to be developing new software, called "Universal Face Workstation," to enable this access.[20]

15. The FBI also has access to many states' Department of Motor Vehicles (DMV) face recognition databases. As reported by the *Washington Post*, 37 states use facial recognition in their DMV databases, and "at least 26 of those allow state local or federal law enforcement agencies to search — or request searches."[21] The FBI has formal agreements with at least 10 of those states,[22] and has been working directly with one state—North Carolina—for at least four years.[23]

---

[16] Jerome M. Pender, FBI, *Statement Before the Senate Judiciary Committee, Subcommittee on Privacy, Technology, and the Law* (July 18, 2012) *available at* http://www.fbi.gov/news/testimony/what-facial-recognition-technology-means-for-privacy-and-civil-liberties.

[17] *Staff Paper: NGI Program Implementation and Transition Update*, 6.

[18] Pender, FBI, *Statement Before the Senate Judiciary Committee, Subcommittee on Privacy, Technology, and the Law*.

[19] *Id.*

[20] *Staff Paper: NGI Program Implementation and Transition Update*, 6.

[21] Craig Timberg & Ellen Nakashima, *State Photo-ID Databases Become Troves for Police*, Wash. Post (June 16, 2013) http://www.washingtonpost.com/business/technology/state-photo-id-databases-become-troves-for-police/2013/06/16/6f014bd4-ced5-11e2-8845-d970ccb04497_story.html.

[22] *Id.*

[23] Mike Baker, *FBI Uses Facial Recognition Technology on DMV Photos*, USA Today (October 13, 2009) http://usatoday30.usatoday.com/tech/news/2009-10-13-fbi-dmv-facial-recognition_N.htm.

16. The FBI's plans for face recognition appear to be broader than mug shot and DMV photos. The Face Recognition Pilot Program MOU between FBI and Hawaii states that full implementation of the program will "permit photo submissions independent of arrests" and "permit bulk submission of photos being maintained at state and federal repositories."[24] The FBI has also stated in a public presentation given at a national biometrics conference that it wants to use its facial recognition system to "identify[] unknown persons of interest from images" and "identify[] subjects in public datasets."[25] In the same presentation, the FBI included a graphic image that implied the Bureau wanted to use facial recognition to be able to track people from one political rally to another.[26]

17. The Bureau states that NGI's face recognition system is "scheduled for full operational capability in the summer of 2014.[27] Upon deployment, "the repository will contain 12 million searchable frontal photos."[28]

18. FBI has released very little information to the public about how it uses face recognition, NGI's face recognition capabilities, or about its state pilot program.

Data Sharing and Database Interoperability

19. IAFIS and NGI have been designed to allow non-FBI users to access the systems through data sharing and database interoperability.

20. FBI exchanges data regularly with more than 18,000 national, state, local and tribal law enforcement agencies.[29] These agencies contribute fingerprints, mug shots, biographic data and

---

[24] *MOU between the FBI and the State of Hawaii Dept. of the Attorney Gen. for the Interstate Photo System Facial Recognition Pilot*, 2, *available at* https://www.eff.org/file/35296#page/2/mode/1up (last visited June 20, 2013).

[25] Richard Vorder Bruegge, *Facial Recognition and Identification Initiatives*, FBI, 5, https://www.eff.org/file/35308#page/5/mode/1up (last visited June 20, 2013).

[26] *Id.* at 4, *available at* https://www.eff.org/file/35308#page/4/mode/1up.

[27] Pender, FBI, *Statement Before the Senate Judiciary Committee, Subcommittee on Privacy, Technology, and the Law*.

[28] *Staff Paper: NGI Program Implementation and Transition Update*, 6.

[29] *FBI Announces Initial Operating Capability for Next Generation Identification System* (March 8, 2011) http://www.fbi.gov/news/pressrel/press-releases/fbi-announces-initial-operating-capability-for-next-generation-identification-system (last visited June 18, 2012).

criminal histories to IAFIS and are able to query the database 24 hours per day and 365 days per year.[30]

21. In the last few years, FBI has been working with various federal agencies, including Department of Homeland Security (DHS), Department of State, and Department of Defense (DOD) to enable the agencies' respective biometrics databases to share data.[31] As noted in a Privacy Impact Assessment (PIA) discussing the plans for interoperability between IAFIS/NGI and DHS's IDENT database, interoperability will achieve "1) enhanced access to, and in some cases acquisition of, the IAFIS/NGI information by the IDENT and its users and 2) the reciprocal enhanced access to, and in some cases acquisition of, the IDENT information by the IAFIS/NGI and its users."[32]

22. Federal database interoperability does not just affect the federal agencies maintaining the individual databases. As of December 31, 2011, 43 states and the territory of Puerto Rico were also able to take advantage of IDENT/IAFIS interoperability.[33]

23. The FBI also shares biometric data with at least 77 countries through formal and informal relationships.[34] The Bureau is in the process of partnering with several "Visa Waiver Program countries" such as Ireland, Spain and Australia to allow each country automatic access to the other's biometric database.[35]

---

[30] *Id.*

[31] Biometrics Identity Management Agency, "The Biometrics Triad: Working to Seamlessly Integrate Biometric Data," *The Biometric Scan*, (Jan.–March 2010) http://www.biometrics.dod.mil/Newsletter/issues/2010/Jan/v6issue1_a4.html (last visited June 24, 2013).

[32] FBI, *Privacy Impact Assessment: Integrated Automated Fingerprint Identification System (IAFIS)/Next Generation Identification (NGI) Biometric Interoperability*, https://www.fbi.gov/foia/privacy-impact-assessments/iafis-ngi-interoperability-1 (last visited June 24, 2013).

[33] *Staff Paper: State Participation in Automated Biometric Identification System (IDENT)/Integrated Automated Fingerprint Identification System (IAFIS) Interoperability*, CJIS Advisory Policy Board (APB) Spring 2012 Advisory Process Meetings https://www.eff.org/file/35291#page/88/mode/1up (last visited June 20, 2013).

[34] *Staff Paper: Biometric Information Sharing Update*, CJIS Advisory Policy Board (APB) Spring 2012 Advisory Process Meetings https://www.eff.org/file/35294#page/2/mode/1up (last visited June 20, 2013).

[35] *Id.*

Civil and Criminal Records

24. In the past, civil and criminal biometric and biographic data were kept separate in IAFIS.[36] This meant that a query to one database would not necessarily produce records from the other.[37]

25. The FBI appears poised to link or combine the civil and criminal records in NGI under a "Master Name" or unique identifier.[38] At a 2012 meeting, the Criminal Justice Information Services (CJIS) Advisory Board—a body "responsible for reviewing appropriate policy, technical, and operational issues" related to programs such as IAFIS[39]—discussed plans to link the records, which could allow system users to search criminal and civil records at the same time. The Board stated that although "all information about a person in the system" would be maintained "as a single record," the system itself would be designed to ensure that "retained civil submissions remain untainted by criminal submissions."[40]

26. FBI has not explained to the public how NGI or IAFIS's system design would ensure that civil submissions are not "tainted" by criminal submissions or explained why it is necessary to combine the two types of data.

Privacy Concerns with IAFIS and NGI

27. Governmental use of face recognition—and the potential for misuse—raises many privacy concerns. As Senator Al Franken noted at a hearing of the Senate Judiciary Subcommittee on Privacy, Technology and the Law last year,

> facial recognition creates acute privacy concerns that fingerprints do not. Once someone has your fingerprint, they can dust your house or your surroundings to figure out what you've touched. Once someone has your faceprint, they can get your name, they can find your social networking

---

[36] *Staff Paper: Implementation of the Next Generation Identification (NGI) Enhanced Repository*, CJIS Advisory Policy Board (APB) Spring 2012 Advisory Process Meetings https://www.eff.org/sites/default/files/filenode/FBI-CJIS-AB_NGI_Master_Name_2012.pdf (last visited June 20, 2013)(hereinafter "*Staff Paper: Implementation of the NGI Enhanced Repository*").

[37] *Id.*

[38] *Id.*

[39] FBI, *The CJIS Advisory Process: A Shared Management Concept*, http://www.fbi.gov/about-us/cjis/advisory-policy-board (last visited June 20, 2013).

[40] *Staff Paper: Implementation of the NGI Enhanced Repository*.

> account and they can find and track you in the street, in the stores you visit, the government buildings you enter, and the photos your friends post online.[41]

Franken went on to note, "I fear that without further protections, this technology could be used on unsuspecting civilians innocent of any crime, or could be used to instantly identify someone walking down the street. I urge the FBI . . . to do more to protect people's privacy so that this new technology isn't abused."[42]

28. The Privacy Impact Assessments (PIAs) for IAFIS and NGI have not kept pace with these programs' development. Five years ago, on June 9, 2008, the FBI published a PIA concerning "enhancements" to the IAFIS Interstate Photo System (IPS).[43] This was only a few months after FBI awarded the NGI contract to Lockheed Martin and well before the FBI developed the face recognition component of NGI as it exists today.

29. Nevertheless, the PIA recognized several privacy risks posed by the enhancements. For example, for some photos, "the subjects may not have been aware of being photographed, and their identities may not yet be known or established." Nevertheless, the PIA noted these photos would still be included in the database. Photographs that could not be identified when submitted would be "maintained in a common photo file." If the individual in the photo is later identified, the photo may later be associated with that individual's file.[44] This means people may have their photograph—and their unique face print—in a government-maintained criminal database without their knowledge. And a certain percentage of these people likely are not engaged in criminal activity.

30. The FBI recognizes that the 2008 Interstate Photo System PIA is outdated and testified before Congress in July 2012 that "an updated PIA is planned and will address all

---

[41] Press Release, *Sen. Franken Presses Facebook, Government to Safeguard Privacy As Facial Recognition Technology Quickly Advances*, (July 18, 2012) http://www.franken.senate.gov/?p=press_release&id=2144.

[42] *Id.*

[43] FBI, *PIA for the NGI IPS*.

[44] *Id.*

evolutionary changes since the preparation of the 2008 Interstate Photo System PIA."[45] However, although the Bureau appears to be accepting photographs from each of the states involved in the pilot program and plans to achieve full deployment of its face recognition program next year, it has yet to release a new PIA.

Technical Limitations of Face Recognition

31. Researchers and government officials have noted that face recognition is not infallible, and is in fact "highly dependent on the quality of images enrolled in the system."[46] It performs well with consistent lighting conditions and poses. However, with variable lighting, shadows, backgrounds, poses or expressions, the error rates are significant.[47] Other factors, such as age of the subject, gender, and race also affect accuracy.[48] Further, as facial recognition databases increase in size, the risk of false positives—such as a person being misidentified as the perpetrator of a crime—increases as well.[49]

32. The FBI recognizes this problem and has proposed to address it in several ways. In the 2008 Interstate Photo System PIA, the FBI noted it planned to analyze and specify "critical

---

[45] Pender, FBI, *Statement Before the Senate Judiciary Committee, Subcommittee on Privacy, Technology, and the Law*.

[46] *Staff Paper: NGI Program Implementation and Transition Update*, 6; *see also* FBI Biometric Center of Excellence, *Face Recognition*, http://www.biometriccoe.gov/Modalities/facialRecognition.htm (last visited June 24, 2013) (noting that "the need for higher accuracy [in face recognition] remains").

[47] *See, e.g.*, P. Jonathon Phillips, et al., *An Introduction to the Good, the Bad, & the Ugly Face Recognition: Challenge Problem*, National Institute of Standards & Testing (Dec. 2011), *available at* www.nist.gov/itl/iad/ig/upload/05771424.pdf (noting only 15% accuracy for face image pairs that are "difficult to match"). Security researcher Bruce Schneier has noted that even a 90% accurate system "will sound a million false alarms for every real terrorist" and that it is "unlikely that terrorists will pose for crisp, clear photos." Bruce Schneier, *Beyond Fear: Thinking Sensibly About Security in an Uncertain World*, 190 (2003).

[48] Patrick J. Grother, et al., *Report on the Evaluation of 2D Still-Image Face Recognition Algorithms*, NIST Interagency Report 7709, 4 (Aug. 24, 2011) *available at* http://www.nist.gov/customcf/get_pdf.cfm?pub_id=905968.

[49] *See, e.g.*, Lucas D. Introna & Helen Nissenbaum, *Facial Recognition Technology: A Survey of Policy and Implementation Issues*, 3, N.Y.U. (April 2009), *available at http://www.nyu.edu/ccpr/pubs/Niss_04.08.09.pdf*; *see also* Grother, *Report on the Evaluation of 2D Still-Image Face Recognition Algorithms*, 26 ("the chance of one or more false matches increases with the population size").

performance parameters . . . through functional and system requirements analysis."[50] It would also "promulgate policies and procedures to emphasize that photographic matches are not to be considered 'positive' identifications, and searches of the photographs will merely result in a ranked listing of candidates."[51] Further, "[u]sers will be trained on system limitations, and to recognize that the aging process and intentional lifestyle choices will reduce the effectiveness of image searching."[52]

33. The FBI has not made this technical information or any of its proposed policies for addressing NGI face recognition's limitations available to the public.

Plaintiff's FOIA Requests

34. Between June 25, 2012 and July 5, 2012, Plaintiff sent three FOIA requests via email to Defendant concerning Defendant's use of facial recognition and development of its Next Generation Identification (NGI) system.

35. Each of these requests sought search, review and duplication fee waivers based on EFF's status as a news media requester and based on the fact that disclosure of the requested information is in the public interest within the meaning of 5 U.S.C. § 552(a)(4)(A)(ii)-(iii). In the requests, EFF presented facts to support its fee waiver requests.

36. Each of these requests also asked that documents be produced in their native file format. Specifically, EFF requested:

a. that files stored in electronic format be produced in electronic format;

b. that files be produced either in their native format (likely appropriate for spreadsheets and database files—for example, Microsoft Excel files produced as .xls electronic files) or as text-searchable pdf formatted files (likely appropriate for word processing documents, letters, memos, or emails);

c. that files preserve the "parent / child" relationship between records (for example, if an email has an attachment, that attachment—or, if appropriate, information

---

[50] FBI, *PIA for the NGI IPS*.
[51] *Id.*
[52] *Id.*

regarding the attachment's withholding—should accompany or follow the pdf of the email); and that the beginning and ending of individual records is clearly indicated.

First Request — FBI/State Facial Recognition Partnerships

37. The first request, dated June 25, 2012, sought records related to the FBI's plans to partner with states to build out its facial recognition database. The request sought all agency records, including electronic records, created from January 1, 2010 to the present concerning FBI's plans to incorporate facial recognition capabilities and face-recognition-ready photographs into NGI. Specifically, it sought records related to:

a. memoranda of understanding (MOUs) or other similar contracts or agreements between the FBI and any states concerning submitting facial recognition photographs to and retrieving or accessing photographs from the Next Generation Identification database;

b. discussions between the FBI and any states regarding the state's participation in a program to submit and/or retrieve facial recognition photographs to the FBI's Next Generation Identification (NGI) database;

c. records related to a "Face Report Card," possibly created by FBI's Next Generation Identification Program Office to "provide feedback to individual agencies regarding the quality of images submitted" to the FBI's Next Generation Identification database.

38. The FBI acknowledged receipt of Plaintiff's request via email dated June 26, 2012 and letter dated July 2, 2012. In the July 2 letter, the FBI stated it had begun the search and was considering EFF's fee waiver request. Defendant also assigned Plaintiff's FOIA request, FOIA Request No. 1193642.

39. In a letter dated October 5, 2012, the FBI stated it had located approximately "7380 pages which are potentially responsive to the FOIA." FBI also noted that EFF's fee waiver request was still under review and requested that EFF convey its "willingness to pay the estimated search and duplication costs" of "$215.00 (15 CD's at $15.00 less $10.00) to receive the release on a CD."

40. By letter dated November 1, 2012 and sent via email, EFF conditionally committed to paying up to $215 to receive records on a CD. EFF stated it did not waive its right to appeal or otherwise contest any decision denying EFF's fee waiver request.

41. FBI has not produced any records in response to EFF's first request.

Second Request — Combining Civil and Criminal Data

42. The second request, dated July 5, 2012, sought records related to FBI's plans to combine civil and criminal data, including biometric data in the Next Generation Identification (NGI) database or Integrated Automated Fingerprint Identification System (IAFIS). The request sought all agency records, including electronic records, created from January 1, 2010 to the present concerning:

a. developing and/or implementing a "Master Name" or unique identity for civil records or civil and criminal records in the IAFIS or NGI databases;

b. combining civil and criminal biometric and biographic records in IAFIS or NGI or another repository and discussions related to migrating to an automated identity management structure that would maintain all information about a person in the system as a single record based on a unique identity;

c. rules or policies that govern or define the sharing or dissemination of civil information once civil and criminal records are stored together in a single repository.

43. The FBI acknowledged receipt of Plaintiff's request via email dated July 6, 2012.

44. FBI has not produced any records in response to EFF's second request.

Third Request — Face Recognition Reliability

45. The third request, dated July 5, 2012, sought records related to the reliability of facial recognition capabilities in the FBI's Next Generation Identification (NGI) database. The request sought all agency records, including electronic records, created from January 1, 2010 to the present concerning:

a. any studies, reports, notes, comments, or other records on the reliability of facial recognition biometric data in the NGI database and/or the Face Recognition Pilot (FRP) project in the NGI database. These studies, reports, etc, could include information on the ability of the database to accurately identify a person in a photograph submitted to the database and/or data on the false-accept rate (FAR) and false-reject rate (FRR) of the database;

b. any information on the total current number of face recognition capable records and/or searchable frontal photographs in the database and the proposed number at deployment;

c. any studies, reports, notes, comments, or other records that discuss specific image quality metrics, best practices, and recommendations regarding quality of images submitted to or enrolled in the system.

46. The FBI acknowledged receipt of Plaintiff's request via email dated July 6, 2012.

47. FBI has not produced any records in response to EFF's third request.

48. Defendant has exceeded the generally applicable twenty-day deadline for the processing of FOIA requests.

49. Plaintiff has exhausted the applicable administrative remedies with respect to all of its FOIA requests referenced herein.

50. Defendant has wrongfully withheld the requested records from Plaintiff.

CAUSES OF ACTION

Violation of the Freedom of Information Act for Wrongful Withholding of Agency Records

51. Plaintiff repeats and realleges paragraphs 1-50.

52. Defendant has wrongfully withheld agency records requested by Plaintiff by failing to comply with the statutory time limit for the processing of FOIA requests.

53. Plaintiff has exhausted the applicable administrative remedies with respect to Defendant's wrongful withholding of the requested records.

54. Plaintiff is entitled to injunctive relief with respect to the release and disclosure of the requested documents.

REQUESTED RELIEF

WHEREFORE, Plaintiff prays that this Court:

1. order Defendant and its components to process immediately the requested records in their entirety;

2. order Defendant and its components to disclose the requested records in their entirety and make copies available to Plaintiff;

3. award Plaintiff its costs and reasonable attorneys fees incurred in this action; and

4. grant such other relief as the Court may deem just and proper.

DATED: June 26, 2013

By _____

Jennifer Lynch, Esq.
ELECTRONIC FRONTIER FOUNDATION
815 Eddy St.
San Francisco, CA 94109

David L. Sobel *(pro hac vice pending)*
ELECTRONIC FRONTIER FOUNDATION
1818 N Street, N.W., Suite 410
Washington, DC 20009

Attorneys for Plaintiff
ELECTRONIC FRONTIER FOUNDATION